Privacy and Mobile Technologies: the Need to Build a Digital Culture

Mathilde de Saint Léger, Sébastien Gambs, Brigitte Juanals, Jean-François Lalande, Jean-Luc Minel

Privacy and Mobile Technologies: the Need to Build a Digital Culture

M. De Saint Léger[1], S. Gambs[2], B. Juanals[1], J.-F. Lalande[2,3], and J.-L. Minel[1]

[1] MoDyCO, UMR 7114, Université Paris-Ouest Nanterre La Défense - CNRS
200 avenue de la République, 92001 Nanterre, France
[2] Université de Rennes 1, Inria, SUPELEC, CNRS, IRISA, UMR 6074
avenue de la Boulaie, 35576 Cesson Sévigné, France
[3] INSA Centre Val de Loire, Univ. Orléans, LIFO, EA 4022
88 bld Lahitolle, 18022 Bourges, France

Abstract. This paper studies the topic of privacy in its relations with mobile technologies. After presenting the complexity of the topic and the need for an interdisciplinary approach on this subject, we analyze its media coverage in the modern public space. Despite the difficulties highlighted by these studies, we argue that research efforts should support the emergence of mobile services that respect users' privacy as well as the development of a digital culture of privacy.

Keywords: privacy, mobile technologies, digital culture, media construction, social appropriation, public space

1 Introduction

Privacy is a concept that is difficult to grasp due to its broad definition and the vast number of disciplinary points of view on this subject, particularly in public and private law, in economy or in political philosophy. Privacy is often addressed in the context of information systems and electronic artefacts, by relating it to the traceability issues raised by the technological possibilities of identifying and tracking people. In this paper, we focus particularly on the topic of mobile technologies and its interactions with the evolution of the regulatory and legal framework at an international level, academic research in computer science and engineering, and the social representations that are being developed around these technologies in the media.

The outline of the paper is the following. First in Section 2, we introduce the complexity of this topic and the need for interdisciplinary study. In Section 3, we present an analysis of the media coverage of the protection of personal data in relation with mobile technologies in the modern public space. Finally, we conclude in Section 4 by calling for the development of a digital culture of privacy for mobile technologies.

2 The Complexity of Privacy for Mobile Technologies

Understanding the technical characteristics of mobile technologies, even if they are used on a daily basis by individuals, requires an in-depth knowledge of computer science, electronics, mathematics and engineering. Moreover, the protection of privacy is as much a technical topic as a political, economic and legal one. In the following, we briefly review the points of view of some of these different actors.

Legal experts. Legal experts are specialists in the analysis of laws (private, public) and study the heterogeneity and relations between different legislations at the national, European or international level. In Europe, the concept of "security and privacy by design", which puts forward the idea that security and privacy should be taken into account as early on as the design phase of a service, is explicitly recommended for the implementation of RFID technologies by the European Commission [1]. In particular, new technologies should incorporate some fundamental privacy principles in their design. For instance, the data minimization principle states that only the information necessary to complete a particular application should be disclosed (and no more) while the data sovereignty principle states that the data related to an individual belong to him and that he should stay in control of how these data are used and for which purpose.

Engineers. Engineers design hardware and software for mobile technologies by taking into account both the regulatory constraints (e.g. with respect to privacy) and the security requirements induced by these technologies. In particular, they propose new easy-to-use services, which at the same time raise strong privacy concerns due to the strong link with the user's identity. Indeed, deploying contactless application on the user's smartphone facilitates the opportunities for an adversary to collect personal data or to track his actions. For example, Near Field Communication (NFC) technology poses security threats such as signal interception, unauthorized access to stored information or traceability of location of the owners of these devices [11].

Computer scientists. In the privacy literature, an increasing number of authors have revisited existing mobile services by developing privacy-preserving variants for them. For instance in the context of transportation systems, novel ticketing systems enable users to validate a ticket using NFC while guaranteeing revocable anonymity for the users [6, 7]. These proposals provide anonymity and unlinkability properties but also offer the possibility of revoking a user (e.g. in the event of fraud).

Within the context of the LYRICS project[4], we have proposed and implemented a privacy-preserving mobile transportation pass [2]. The prototype developed takes the form of a cardlet stored in a SIM card that communicates by NFC with a validator at the entrance gate of a transportation system. The user

[4] ANR-11-INS-0013 LYRICS project: http://projet.lyrics.orange-labs.fr

shows his smartphone at the gate to validate his digital transportation pass. In such a use case, there is a strong risk that the trips of a user will be tracked by the transportation authority. To counter this threat, we have designed a validation protocol based on group signatures making it possible to sign anonymously, in less than 300ms, a challenge sent by the gate to prove the validity of the pass. The group signature preserves the anonymity of the user and the unlinkability of two different signatures, thus preventing the possibility of tracking the whereabouts of a user.

Users. From the perspective of the standard user, novel privacy-enhancing technologies, while providing strong privacy guarantees, are not necessarily easy to understand. Indeed, their complexity calls for a much greater effort at explanation, similar to what has been conducted for mature technologies such as the certification of web pages using the HTTPS protocol. Addressing this issue adequately requires first understanding the social appropriation of mobile technologies and how users feel about their privacy-preserving variants. To achieve this, one should first assess the evolutions and the societal implications of the appropriation of mobile technologies by the public. The next section presents the result of our analysis that relies on field investigations in computer science, science engineering and social sciences.

3 The Media Construction of the Societal Question of Privacy in Mobile Technologies

This section addresses the analysis of the media coverage of privacy in relation with mobile technologies in the modern public space. More precisely, our analysis follows the lines of studies devoted to transformations of the public space and the mutations of media [12, 14]. We study the relations between the media and the social construction of privacy in mobile technologies, in the public space, as a complex social and political construction within an international "force field" [3]. We formulate the hypothesis that the role of the media in the understanding of the topic and the coverage of practices of organisations play an active part in the construction of modes of protection of personal data [8]. Our corpus is composed of 569 newspaper articles and 990 comments collected from seven French generic and professional newspapers and three blogs of journalists over the period 2012-2013. To process such a large amount of data, we designed a partially instrumented qualitative and quantitative methodology relying on open access natural language processing and data mining tools (TXM, Calliope and Gephi). First, our workflow harvests the web before performing a lexicometric [13, 9] and a clustering analysis [10, 4].

From the results of this study, we wish to emphasize the following points. First, the lexicometric analysis, and more specifically the index of specificity [9], shows that the stakeholders that are the most frequently mentioned are: Google, the CNIL, Apple and the European Commission in generic newspapers, Orange in professional ones and Facebook in the blogs. Thus, American companies are

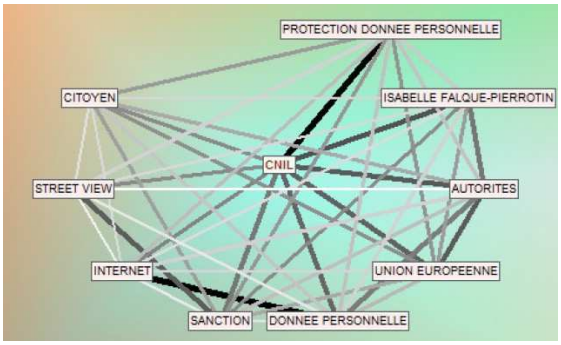

Fig. 1. Example of semantic universe

the stakeholders that are the most publicized to the detriment of public organisations in charge of regulatory systems with the exception of the CNIL and the European Commission. The clustering analysis, and more specifically the analysis of semantic universes of computed clusters [5] further demonstrates that generic newspapers associate privacy issues with the non-compliance of European rules by American companies (Google, Facebook). In addition, the professional newspapers provide factual comment on mobile products and services, with little critical analysis. News items are characterized by the heavy advertising presence of telecommunications companies (mobile manufacturers, telecom operators), which is the consequence of this mode of media coverage. Public organisations in charge of regulatory systems (CNIL, the European Commission) are mainly mentioned for their role of imposing sanctions (cf. Figure 1). Finally, showing a greater proximity with their readers, blogs focus on day-to-day problems experienced about privacy issues in mobile technologies. The discursive analysis of readers' comments shows a rejection and a clear lack of trust towards companies related to mobile technologies. Thus, there is a wide gap between media discourse and the hostile reactions of readers.

4 Developing a Digital Culture of Privacy

To summarize, the main results of this study are that 1) American companies are the stakeholders that are the most publicized to the detriment of public organisations in charge of privacy regulations; 2) generic newspapers associate most of the privacy issues in mobile technologies with the non-compliance of European regulations by American companies; 3) professional newspapers are rather factual than critical towards new mobile technologies and services. Based on these conclusions, we think that a considerable effort needs to be made to support the emergence of privacy-preserving mobile services. As an example, we have briefly described a prototype of a contactless transportation pass designed

to improve the protection of personal data when embedded in a smartphone developed within the LYRICS project [2].

To conclude, we believe that there is a serious discrepancy between the apprehension and the understanding of privacy in mobile technologies. We interpret this discrepancy as an indication of the lack of a digital culture on this subject, both by journalists and the general public. In particular, individuals face the consequences of the use of mobile devices of which the privacy is impacted by technologies and norms (standards, laws, regulations) that they are little aware of. Nevertheless, these artefacts are increasingly posing societal, ethical and political challenges and call for interdisciplinary studies and public debate on this topic. In this respect, a digital culture of privacy for mobile technologies remains to be developed.

References

1. Commission recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. Tech. rep., European Commission, Brussels (2009)
2. Arfaoui, G., Gambs, S., Lacharme, P., Lalande, J.F., Roch, L., Paillès, J.C.: A Privacy-Preserving Contactless Transport Service for NFC Smartphones. In: Fifth International Conference on Mobile Computing, Applications and Services. LNICST, Springer Berlin / Heidelberg, Paris, France (Nov 2013)
3. Chateauraynaud, F.: Argumenter dans un champ de forces. Essai de balistique sociologique. Pétra edn. (2011)
4. de Saint Léger, M.: Modélisation de la dynamique des flux d'information par le bruit. Ph.D. thesis, CNAM, Paris (1997)
5. de Saint Léger, M., van Meter, K.: Cartographie du premier congrès de l'ASF avec la méthode des mots associés. Bulletin de méthodologie sociologique 85, 44–67 (2005)
6. Derler, D., Potzmader, K., Winter, J., Dietrich, K.: Anonymous Ticketing for NFC-Enabled Mobile Phones. In: Chen, L., Yung, M., Zhu, L. (eds.) The Third International Conference on Trusted Systems. vol. 7222, pp. 66–83. Beijing, China (2011)
7. Isern-Deya, A.P., Vives-Guasch, A., Mut-Puigserver, M., Payeras-Capella, M., Castella-Roca, J.: A Secure Automatic Fare Collection System for Time-Based or Distance-Based Services with Revocable Anonymity for Users. The Computer Journal 56(10), 1198–1215 (Apr 2012)
8. Juanals, B., Minel, J.L.: Construction d'une approche interdisciplinaire et expérimentale pour l'analyse de la communication d'influence. ESSACHESS Journal for Communication Studies 6(1), 187–200 (2013)
9. Lafon, P.: Sur la variabilité de la fréquence des formes dans un corpus. Mots 1(1), 127–165 (1980)
10. Lebart, L., Salem, A.: Statistique textuelle. Dunod (1994)
11. Madlmayr, G., Langer, J., Kantner, C., Scharinger, J.: NFC Devices: Security and Privacy. In: Third International Conference on Availability, Reliability and Security. pp. 642–647. IEEE Computer Society, Barcelona, Spain (Mar 2008)
12. Miège, B.: L'espace public contemporain. PUG (2010)
13. Muller, C.: Principes et méthodes de statistique lexicales. Hachette Université, Paris (1977)
14. Pailliart, I.: L'Espace public et l'emprise de la communication. Ellug (1995)